

PENDING CLAIMS AS AMENDED

Please amend the claims as follows:

1. (Currently Amended) A method for secure transmissions, the method comprising:
determining a registration key specific to a mobile station participating participant in a transmission;
determining a first key;
encrypting the first key with the registration key;
sending the encrypted first key to the mobile station participating participant in the transmission;
determining a second key for decrypting content on a broadcast channel;
updating the first key after a first time period has elapsed; and
updating the second key after a second time period has elapsed, wherein the updated second key is determined based on ~~updated in~~ two parts, a first part comprising the updated first key known to the participant in the transmission and a second part based on information sent on the broadcast channel, and wherein the first part and the second part are concatenated to determine the updated second key using a cryptographic function.
2. (Currently Amended) The method as in claim 1, wherein ~~updating further comprises:~~
~~—— updating the first key according to a first time period; and~~
~~—— updating the second key according to a second time period, wherein the second~~ time period is less than the first time period.
3. (Currently Amended) The method as in claim 2, wherein updating the first key further comprises[[:]] encrypting an updated first key with the registration key.
4. (Original) The method as in claim 2, further comprising:
encrypting a broadcast stream of information using the second key; and
transmitting the encrypted broadcast stream of information.

5. (Original) The method as in claim 4, wherein the broadcast stream of information comprises video information.

6. (Original) The method as in claim 4, wherein the broadcast stream of information comprises Internet Protocol packets.

7. (Original) The method as in claim 3, further comprising:
calculating a registration key information message; and
transmitting the registration key information message.

8. (Currently Amended) The method as in claim 7, further comprising:
calculating a first key information message corresponding to the updated ~~and~~
~~encrypted~~ first key; and
transmitting the first key information message.

9. (Previously Presented) The method as in claim 8, further comprising:
determining a second key information message corresponding to the updated
second key; and
transmitting the second key information message.

10. (Previously Presented) The method as in claim 1, further comprising:
transmitting the encrypted first key.

11. (Currently Amended) A method for secure reception of a transmission, the method comprising:

receiving a registration key specific to a mobile station participating participant in a transmission;

receiving a first key encrypted with the registration key;

decrypting the first key with the registration key;

determining a second key using a cryptographic function and the first key, for decrypting content on a broadcast channel;

receiving a broadcast stream of information;

decrypting the broadcast stream of information using the second key;

receiving an updated first key after a first time period has elapsed; and

determining an updated second key after a second time period has elapsed, wherein the updated second key is determined based on updated in two parts, a first part comprising the updated first key ~~known to the participant in the transmission~~ and a second part based on information sent on the broadcast channel, and wherein the first part and the second part are concatenated to determine the updated second key using a cryptographic function.

12. (Original) The method as in claim 11, further comprising:

storing the first key in a secure memory storage unit; and

storing the second key in a memory storage unit.

13. (Currently Amended) The method as in claim 11, further comprising:

recovering the updated first key from a first key information message; and

determining the updated second key using a second key information message.

14. (Canceled).

15. (Currently Amended) In a wireless communication system supporting a broadcast service option, an infrastructure element comprising:

a receive circuitry adapted to receive a registration key specific to a mobile station participating participant in a transmission; receive a first key encrypted with the registration key, receive an updated first key after a first time period has elapsed, and receive a second part for updating a short-time key after a second time period has elapsed, ~~wherein the short time key is updated in two parts, a first part known to the participant in the transmission and the second part sent on the broadcast channel;~~

a user identification unit, operative to determine an updated short-time key for decrypting a broadcast message, wherein the short-time key is determined based on two parts, a first part comprising the updated first key and the second part based on information sent on the broadcast channel, and wherein the first part and the second part are concatenated to determine the updated short-time key using a cryptographic function, comprising:

processing unit operative to decrypt and to determine key information;

memory storage unit for storing a registration key; and

a mobile equipment unit adapted to apply the short-time key for decrypting the broadcast message.

16. (Original) The infrastructure element as in claim 15, wherein the short-time key is processed by the user identification unit and passed to the mobile equipment unit.

17. (Original) The infrastructure element as in claim 15, wherein the memory storage unit is a secure memory storage unit.

18. (Currently Amended) The infrastructure element as in claim 15, wherein the memory storage unit stores a broadcast access key comprising the first key, and wherein the processing unit determines the short-time key using the broadcast access key.

19. (Original) The infrastructure element as in claim 18, wherein the short-time key is updated at a first frequency.

20. (Original) The infrastructure element as in claim 19, wherein the broadcast access key is updated at a second frequency less than the first frequency.

21. (Original) The infrastructure element as in claim 15, wherein the broadcast service option is a video service.

22. (Currently Amended) A wireless communication system, comprising:
means for determining a registration key specific to a mobile station participating participant in a transmission;
means for determining a first key;
means for encrypting the first key with the registration key;
means for sending the encrypted first key to the mobile station participating participant in the transmission;
means for determining a second key for decrypting content on a broadcast channel;
means for updating the first key after a first time period has elapsed; and
means for updating the second key after a second time period has elapsed, wherein the updated second key is determined based on ~~updated in~~ two parts, a first part comprising the updated first key known to the participant in the transmission and a second part based on information sent on the broadcast channel, and wherein the first part and the second part are concatenated to determine the updated second key using a cryptographic function.

23. (Currently Amended) An infrastructure element, comprising:

means for receiving a registration key specific to a mobile station participating participant in a transmission;

means for receiving a first key encrypted with the registration key;

means for decrypting the first key with the registration key;

means for determining a second key using a cryptographic function and the first key, for decrypting content on a broadcast channel;

means for receiving a broadcast stream of information;

means for decrypting the broadcast stream of information using the second key;

means for updating the first key after a first time period has elapsed; and

means for updating the second key after a second time period has elapsed, wherein the updated second key is determined based on ~~updated in~~ two parts, a first part comprising the updated first key known to the participant in the transmission and a second part based on information sent on the broadcast channel, and wherein the first part and the second part are concatenated to determine the updated second key using a cryptographic function.

24. (Currently Amended) A digital storage device, comprising:

- first set of instructions for receiving a registration key specific to a mobile station participating participant in a transmission;
- second set of instructions for receiving a first key encrypted with the registration key;
- third set of instructions for decrypting the first key with the registration key;
- fourth set of instructions for determining a second key using a cryptographic function and the first key, for decrypting content on a broadcast channel;
- fifth set of instructions for receiving the broadcast stream of information;
- sixth set of instructions for decrypting the broadcast stream of information using the second key; and
- seventh set of instructions for updating the first key after a first time period has elapsed, updating the second key after a second time period has elapsed, wherein the updated second key is determined based on updated in two parts, a first part comprising the updated first key known to the participant in the transmission and a second part based on information sent on a broadcast channel, and wherein the first part and the second part are concatenated to determine the updated second key using a cryptographic function.

25. (Currently Amended) The digital storage device as in claim 24, wherein the second first part is further based on ~~includes~~ a time value.

26. (Currently Amended) The digital storage device as in claim 24, wherein the updated second key is determined by applying a cryptographic hash function to the concatenation of the first and second parts.

27. (Currently Amended) The method as in claim 1, wherein the second first part is further based on ~~includes~~ a time value.

28. (Currently Amended) The method as in claim 1, wherein the updated second key is determined by applying a cryptographic hash function to the concatenation of the first and second parts.

29. (Currently Amended) The method as in claim 11, wherein the second first part is further based on ~~includes~~ a time value.

30. (Currently Amended) The method as in claim 11, wherein the updated second key is determined by applying a cryptographic hash function to the concatenation of the first and second parts.

31. (Currently Amended) The infrastructure element as in claim 15, wherein the second first part is further based on ~~includes~~ a time value.

32. (Currently Amended) The infrastructure element as in claim 15, wherein the updated short-time key is determined by applying a cryptographic hash function to the concatenation of the first and second parts.

33. (Currently Amended) The wireless communication system as in claim 22, wherein the second first part is further based on ~~includes~~ a time value.

34. (Currently Amended) The wireless communication system as in claim 22, wherein the updated second key is determined by applying a cryptographic hash function to the concatenation of the first and second parts.

35. (Currently Amended) The infrastructure element as in claim 23, wherein the second first part is further based on ~~includes~~ a time value.

36. (Currently Amended) The infrastructure element as in claim 23, wherein the updated second key is determined by applying a cryptographic hash function to the concatenation of the first and second parts.

PATENT

37. (New) The method as in claim 27, wherein the time value is not sent on the broadcast channel.

38. (New) The method as in claim 29, wherein the time value is not sent on the broadcast channel.

39. (New) The infrastructure element as in claim 31, wherein the time value is not sent on the broadcast channel.

40. (New) The wireless communication system as in claim 33, wherein the time value is not sent on the broadcast channel.

41. (New) The infrastructure element as in claim 35, wherein the time value is not sent on the broadcast channel.

42. (New) The digital storage device as in claim 25, wherein the time value is not sent on the broadcast channel.